아르키움(ARX)

주요내용설명서(국문백서)

Korean White Paper

2026년 6월 26일

Disclaimer

본 번역본은 2026년 6월 26일 기준의 아르키움(ARX) 홈페이지 및 X(구 트위터)의 관련 내용 위주로 번역됐습니다.

빗썸은 발행주체 또는 운영주체가 제공하는 가상자산의 총발행량, 유통량 계획, 사업 계획 등이 포함된 정보를 이용자들의 편의를 위해 참고용으로 제공하고 있습니다.

본 번역본은 그 내용이 정확하지 않을 수 있으며 원문의 내용이 일부 누락될 수 있으므로, 정확한 정보 습득을 위해서는 원문을 참고하시거나 원문 작성 측에 문의하시기를 바랍니다. 또한 본 번역본은 오픈 커뮤니티의 검토에 따라 내용이 변경될 수 있습니다.

빗썸

프로젝트 소개

아르키움(Arcium)은 블록체인 기반의 기밀 컴퓨팅[1] 기능을 제공하는 빠르고 유연하며 비용 효율적인 인프라입니다. 아르키움은 '기밀 슈퍼컴퓨터(Confidential Supercomputer)'로서 데이터의 기밀을 완전히 유지한 채로 연산할 수 있는 검증 가능하고 효율적인 무신뢰[2] 프레임워크를 활용하여 개발자, 애플리케이션 및 모든 산업 분야에 기밀 컴퓨팅 실행을 대규모로 지원할 수 있습니다. 보안이 뛰어난 다자간 연산[3] 기술과 탈중앙화 네트워크를 통해 작동하는 아르키움은 웹2.0와 웹3.0를 위한 확장 가능하고 안전한 기밀 솔루션을 제공합니다.

주요 이점

기밀성과 관련해서 프로젝트 및 사용자가 취할 수 있는 주요 이점은 세 가지입니다.

- 완전한 기밀성: 모든 신규 및 기존 애플리케이션의 사용자들에게 무신뢰 방식으로 완전한 기밀성이 보장됩니다.
- 더욱 강력한 앱 개발 가능: 데이터의 기밀 상태를 완벽하게 유지하여 데이터를 연산하는 것이 가능하며, 이를 활용해 새로운 온체인 및 오프체인 애플리케이션이 개발될 수 있는 가능성이 열리게 됩니다.
- 손쉬운 통합: 단 몇 줄의 코드만으로 기밀 컴퓨팅 기능을 원활하게 통합할 수 있습니다.

아르키움의 무신뢰 접근 방식과 검증 가능한 연산을 통해 AI, 디파이[4], 디핀[5]을 비롯한 모든 분야에서는 데이터 보안을 강화할 뿐만 아니라 완전히 새로운 사용 사례와 애플리케이션을 구현할 수 있습니다. 이러한 관점에서 아르키움은 데이터의 중요성이 점점 커져가는 시대에 걸맞은 이상적인 탈중앙화 보안 연산 솔루션이라 할 수 있습니다.

[1] Confidential computing

[2] Trustless

[3] Multi-party computation (MPC)

[4] DeFi (decentralized finance)

[5] DePIN (dencentralized physical infrastructure network)

비즈니스 모델

핵심 특징

아르키움이 최첨단 보안 연산 솔루션일 수 있는 것은 아래와 같은 핵심적인 특징들 덕분입니다.

- 무신뢰·무작위 기밀 컴퓨팅: 기밀 데이터를 노출시키지 않고 임의로 연산하는 다자간 연산 실행 환경(MPC eXecution Environment, MXE)을 활용하여 특정 주체에 대한 신뢰가 필요치 않습니다.
- 실행 보장: 블록체인 기반의 조정 시스템을 활용함으로써 MXE에서 이루어지는 모든 연산 작업을 안정적으로 처리합니다. 아르키움은 네트워크가 규칙에 따라 운영될 수 있도록 스테이킹[6] 및 삭감[7] 메커니즘을 적용합니다. 따라서 노드[8]는 담보를 예치해야 하며, 실행 규칙에 어긋나게 행동할 시 담보에 불이익이 발생하게 됩니다. 이러한 과정을 통해 모든 연산이 정확하게 완료되도록 보장합니다.
- 검증 가능성 및 기밀성: 아르키움에서 제공하는 검증 가능한 연산을 위한 메커니즘을 바탕으로 참여자는 연산 결과의 정확성을 공개적으로 검증할 수 있습니다.
- 온체인 조정: 아르키움은 솔라나 블록체인을 활용하여 노드 작업 일정, 보상 및 성과 인센티브를 관리합니다. 스테이킹과 삭감, 기타 인센티브 또한 완전히 온체인에서 이루어집니다.
- 개발자 친화적 인터페이스: 아르키움은 이중 인터페이스를 제공합니다. 하나는 비전문가가 쉽게 사용할 수 있는 웹 기반의 그래픽 인터페이스이며, 다른 하나는 개발자가 맞춤 애플리케이션을 생성하는 데 활용할 수 있는 솔라나 호환 SDK(소프트웨어 개발 키트)[9]입니다. 두 가지의 인터페이스를 마련하여 일반 사용자와 전문 개발자 모두가 기밀 컴퓨팅을 쉽게 접할 수 있도록 합니다.
- 멀티체인: 아르키움은 우선적으로 솔라나를 기반으로 하고 있지만 멀티체인 호환이 가능하도록 설계되어 있습니다.

위와 같은 특장점을 토대로 아르키움은 민감한 데이터를 무신뢰 환경에서 처리하고 공유하는 방식을 새롭게 정의함으로써, 보안이 뛰어난 다자간 연산 기술을 더욱 널리 전파하고 데이터 기밀성과 보안을 중심으로 하는 새로운 시대를 만들어 가고자 합니다.

[6] Staking

[7] Slashing

[8] Node

[9] Software development kit (SDK)

사용 사례

아르키움을 활용하면 거의 모든 사용 사례에 기밀 컴퓨팅을 적용할 수 있습니다.

- 기밀 디파이: 개발자는 사용자의 기밀성이 보장되는 디앱을 개발하여 보안과 투명성을 모두 확보하면서도 트랜잭션과 스마트 컨트랙트[10] 상호 작용을 비공개 방식으로 처리할 수 있습니다.
- 데이터 분석 협업: 여러 기관에서 민감한 원시 데이터를 서로 공유하지 않고 기밀을 유지한 채로 데이터 연산을 진행하여 유의미한 결과값을 산출할 수 있습니다. 이러한 방식은 데이터 기밀성이 중요한 의료 혹은 금융 분야에 적합합니다.
- AI 모델 보안 학습: 여러 기관이 AI 모델 학습을 위해 협업할 시, 각 기관의 자체 기밀 데이터를 공개하지 않고도 모델을 학습시킬 수 있습니다.
- 다크 풀[11]: 아르키움의 다자간 연산 기술을 활용해 무신뢰 다크 풀을 생성하여 민감한 거래 정보를 공개하지 않고 거래를 진행함으로써 트랜잭션의 기밀성을 유지하고 시장 조종, 프론트 러닝[12] 등의 문제를 예방할 수 있습니다. 대량 거래, 장외 거래와 같은 사용 사례 또한 지원 가능합니다.
- 기관 채택: 작업의 검증 가능성과 확실한 실행을 보장하는 아르키움은 민감한 데이터를 처리하거나 기밀 트랜잭션이 필요한 대형 기관에 안전한 인프라를 제공합니다.
- 기밀 마켓플레이스 및 경매: 참여자는 신원이나 트랜잭션 세부 내용을 밝히지 않고 경매에 참여하여 거래할 수 있습니다. 기밀 기술을 적용한다면 판매자와 구매자 모두를 시장 조종으로부터 보호하는 것이 가능합니다.
- 공급망 관리: 공급망 전반에 걸쳐 민감한 비즈니스 데이터를 보호하면서도 협업할 수 있습니다. 예를 들어 제조 업체와 공급 업체는 가격 책정 및 재고 데이터를 안전하게 공유하는 것 외에도 데이터를 합동으로 연산하여 최적의 생산 일정을 수립하거나 수요를 예측할 수 있습니다. 이 과정에서 입력되는 데이터 값은 상대방에게 공개되지 않습니다. 따라서 민감한 데이터의 기밀을 유지하면서도 공급망 내에서 함께 효율적으로 의사 결정을 내릴 수 있습니다.
- 의료 데이터: 여러 의료 서비스 제공자는 환자 데이터의 기밀을 유지하면서도 데이터를 공동으로 활용할 수 있습니다. 이를 통해 미국 의료 정보 보호법[13]과 같은 규제를 준수하면서 더욱 심층적인 의학 연구를 진행하거나 치료법을 개선할 수 있습니다.

[10] Smart contract

[11] Dark pool

[12] Front running

[13] Health Insurance Portability and Accountability Act (HIPAA)

핵심 개념

기밀 슈퍼컴퓨터 이해하기

아르키움의 역량과 기능을 모두 아우를 수 있도록 아르키움 팀은 아르키움을 '기밀 슈퍼컴퓨터'라고 묘사합니다. 기존의 연산 기술 스택[14]과 유사하게 아르키움의 모든 노드는 프로세서 역할을 하면서 아르키움이라는 하나의 기밀 슈퍼컴퓨터에 기여하게 됩니다. 아르키움 네트워크 내에서 각각의 프로세서들이 결합하고 통합됨으로써 아르키움만의 고유한 특징들이 구체화됩니다. 아르크스OS(arxOS)는 분산형 기밀 운영 시스템(아르키움 노드 네트워크)으로, 연산 실행을 담당합니다. MXE는 아르키움 슈퍼컴퓨터의 VM[15]으로, 자유로운 설정이 가능하며 연산 작업을 안전하게 정의하고 실행할 수 있는 공간이 되어 줍니다. 마지막으로 아르시스(Arcis)는 러스트[16] 기반의 개발 프레임워크입니다.

아르키움과 아르크스 노드(Arx node)

아르키움은 기밀 데이터를 연산하는 탈중앙화 아르크스 노드들로 구성되어 있습니다. '요새'를 뜻하는 라틴어 아르크스(arx)를 차용하여 이름 붙인 아르크스 노드는 하나하나가 아르키움 네트워크의 보안 주체입니다. 하지만 아르크스 노드의 진정한 힘은 탈중앙화 네트워크 기반의 협업에서 비롯됩니다.

- 스테이킹 및 삭감: 네트워크 무결성 보장 차원에서 아르크스 노드는 담보를 스테이킹해야 합니다. 부정 행위 혹은 규칙 위반 시 스테이킹 토큰 삭감 등의 불이익이 가해질 수 있습니다. 이러한 장치를 통해 노드가 정직하게 활동하면서 네트워크의 보안을 유지하도록 유도합니다.

다자간 연산

다자간 연산은 아르키움 암호화 기술의 핵심입니다. 다자간 연산을 통해 복수의 주체가 함께 연산 작업을 수행하면서도 각자 입력한 데이터 값의 비공개 상태를 유지할 수 있습니다. 결과적으로 연산 과정 전반에서 데이터 기밀성이 준수됩니다.

- 비밀 공유[17]는 다자간 연산을 위해 활용되는 주요 암호화 기법으로 데이터를 여러 조각으로 분할하여 다수의 아르크스 노드로 분산시킵니다. 따라서 개별 노드가 전체 데이터를 파악하는 것이 불가능합니다.
- 임계값 암호화[18]는 승인된 주체들 중 일정한 최소 인원이 참여해야만 데이터를 공개할 수 있게 하는 기술입니다. 아르키움은 임계값 암호화를 활용하여 연산 실행 시 데이터 공개를 위해서는 특정 수의 노드가 참여해야 한다는

[14] Technology stack

[15] Virtual machine

[16] Rust

[17] Secret sharing

[18] Threshold encryption

조건을 설정함으로써 민감한 데이터를 보호합니다. 이를 통해 합동으로 연산을 진행하는 경우 보안을 강화할 수 있습니다.

무신뢰 실행

아르키움에서는 무신뢰 방식으로 연산이 실행됩니다. 이는 데이터 처리 과정의 무결성을 검증하는데 그 어떠한 중앙화 주체도 필요치 않음을 뜻합니다. 그 대신 다자간 연산과 같은 암호화 메커니즘을 활용해 연산의 정확성을 확보합니다. 노드는 네트워크 참여를 위해 담보를 스테이킹해야 하며, 규칙 위반 시 불이익을 당할 수 있습니다(스테이킹 토큰 삭감 등). 아르키움의 무신뢰 시스템은 데이터의 기밀을 유지하고 연산 결과의 정확성을 보장합니다.

클러스터(Cluster)와 MXE

아르키움에서 클러스터는 협업하여 다자간 연산 작업을 실행하는 아르크스 노드들의 집합을 의미합니다. 모든 연산 작업은 MXE에서 관리되게 되는데, MXE에는 데이터 처리 방식, 보안 프로토콜, 처리 클러스터 지정 등 연산 작업에 필요한 매개변수들이 설정되어 있습니다. 보통 단일 클러스터는 여러 MXE를 동시에 지원하기 때문에 효율적으로 리소스를 사용하고 작업을 분배할 수 있습니다. 또한 MXE는 여러 클러스터를 활용하도록 설정하는 것이 가능하여, 특정 클러스터가 너무 바쁘거나 일시적으로 작동을 멈추더라도 다른 클러스터로 작업을 이관하여 처리할 수 있습니다. 따라서 높은 수준의 가용성과 유연성이 보장됩니다.

BFT(비잔틴 장애 허용)[19]

아르키움은 BFT를 적용하여 설계되어 악의적으로 행동하거나 작동을 멈춘 노드가 있는 경우에도 정상적으로 운영될 수 있습니다. BFT는 일부 노드가 예측 불가능한 방식으로 행동한다 하더라도 네트워크를 안전하게 가동시킴으로써 탈중앙화 환경에서 신뢰를 보장하고 지속적인 운영을 가능하게 합니다.

에포크[20]

아르키움의 시간은 일정한 시간의 길이를 나타내는 에포크로 구성되어 있습니다. 에포크는 연산 작업 일정을 조율하고 보상을 분배하며 토큰 락업[21] 기간을 관리하기 위한 일종의 시간 체계입니다. 일정한 에포크를 시간 단위로 활용하여 네트워크 작업을 효율적이면서도 공정하게 처리합니다.

[19] Byzantine fault tolerance

[20] Epoch

[21] Lockup

토크노믹스

토큰 개요

네이티브 토큰[22]인 아르키움(ARX)은 네트워크 사용 수수료 결제, 네트워크 보호, 연산 작업 조율, 프로토콜 개발 관리에 활용됩니다. 네트워크가 성장할수록 ARX의 가치 또한 상승합니다.

- 스테이킹: ARX는 노드 운영자가 네트워크에 연산 리소스를 제공하기 위해 예치해야 하는 담보로 활용됩니다. 노드가 연산 리소스를 많이 제공할수록 그만큼 더 많은 ARX를 스테이킹해야 합니다. 따라서 ARX는 네트워크 내 공급자로 참여하기 위해 필요한 수단이라고 할 수 있습니다.
- 거버넌스: ARX는 두 가지 유형의 네트워크 거버넌스에 대한 의사 결정 수단으로 활용됩니다. 토큰을 오래 락업할수록 투표권이 많아집니다.

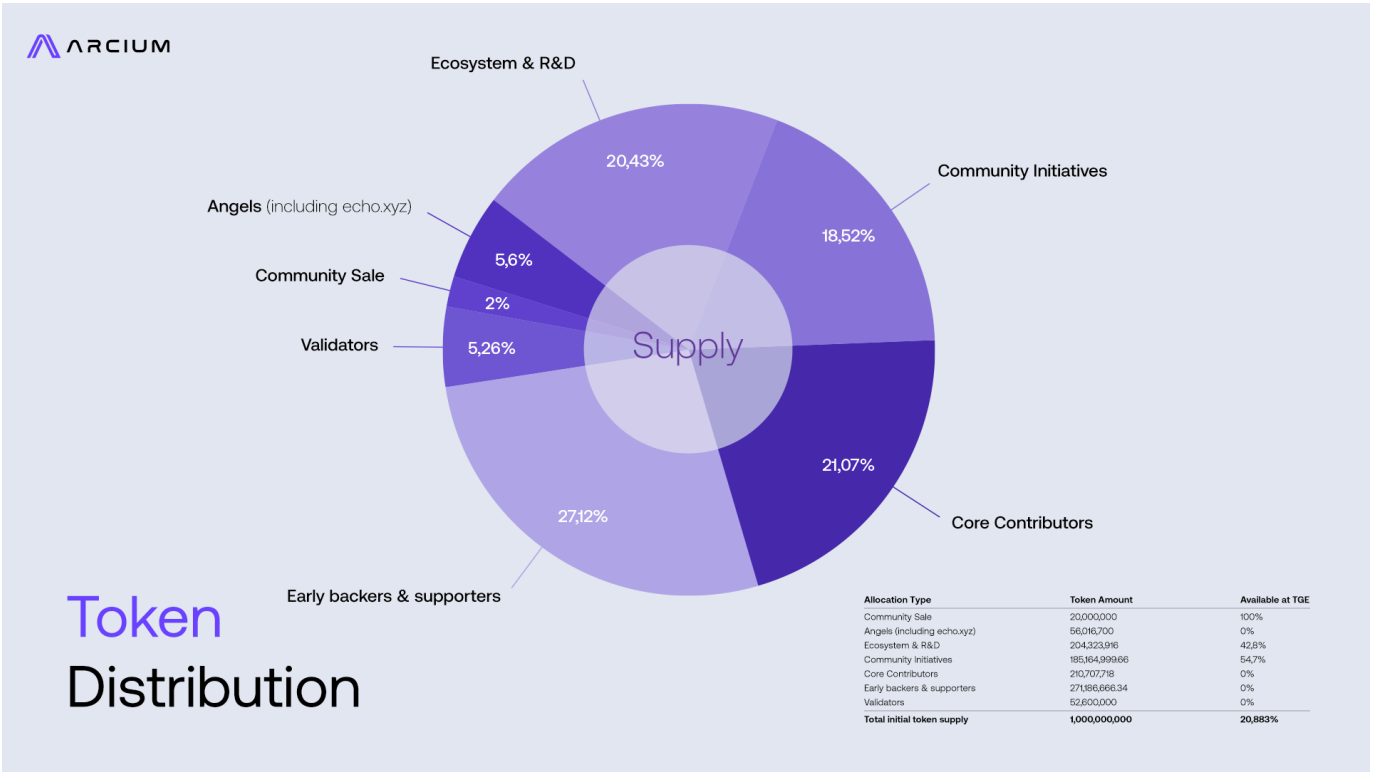
토큰 분배

- 총발행량: 1,000,000,000 ARX
    - 커뮤니티: 20.52%(코인리스트[23] 세일에 2% 할당)
    - 엔젤 투자자(에코[24] 세일 포함): 5.60%
    - 검증인: 5.26%
    - 핵심 기여자: 21.07%
    - 초기 투자자: 27.12%
    - 생태계 및 연구 개발: 20.43%

[22] Native token

[23] CoinList

[24] Echo



[ARX 토큰 분배 그래프]

출시 시점에 총발행량 중 20.883%가 언락[25] 및 유통됩니다. 나머지 79.117%는 출시 시점에 락업되며 사전 설정된 언락 및 베스팅[26] 일정에 따라 유통됩니다. 투자자 및 기여자 할당분에는 토큰 언락 전 12개월의 클리프[27]가 적용됩니다. 초기 총발행량은 출시 시점 이후 약 4년 반 이후에 모두 언락될 것으로 예상됩니다.

[25] Unlock

[26] Vesting

[27] Cliff

[ARX 베스팅 일정 그래프]

로드맵

아르키움은 별도 로드맵을 공지하고 있지 않으나, 공식 홈페이지 및 X(구 트위터)를 통해 사업 현황에 대한 공지를 상시로 진행하고 있습니다.

- 홈페이지: https://www.arcium.com/
- X(구 트위터): https://x.com/Arcium

*상기 링크는 작성일 기준으로 유효한 링크이며 변경될 가능성이 있습니다.